

- 1 1. A method of creating a digital certificate revocation list (CRL), comprising:
2 creating a list of digital certificates satisfying at least one inactive criterion;
3 identifying a latest CRL in which changes have been made to the list; and
4 storing an identity of the latest CRL in which changes have been made as
5 a part of the CRL.
- 6
- 7 2. The method according to claim 1, further comprising formatting as an ASN.1
8 format CRL with the identity of the latest CRL in which changes have been made
9 to the list as an extension to the format.
- 10
- 11 3. The method according to claim 1, wherein the identifying comprises
12 comparing the list with entries in a previously generated CRL.
- 13
- 14 4. The method according to claim 1, wherein the creating, identifying and
15 storing are carried out at regular time intervals.
- 16
- 17 5. The method according to claim 1, further comprising applying a digital
18 signature to the CRL.
- 19
- 20 6. An electronic storage medium storing instructions which when executed on
21 a programmed processor carry out the method of creating a digital certificate
22 revocation list according to claim 1.
- 23
- 24 7. The method according to claim 1, wherein the at least one inactive criterion
25 comprises at least one of a hold status criterion, an expired status criterion and a
26 revoked status criterion.
- 27
- 28 8. The method according to claim 1, further comprising transmitting the CRL
29 to a recipient over an electronic communication medium.
- 30

- 1 9. A method of using a digital certificate revocation list (CRL), comprising:
2 storing a first CRL, the first CRL comprising at least a list of digital
3 certificates satisfying at least one inactive criterion and a first CRL identifier ;
4 carrying out a processing operation on the first CRL;
5 receiving a second CRL, the second CRL comprising at least a list of digital
6 certificates satisfying the at least one inactive criterion, a second CRL identifier and
7 an identity of a latest CRL having differences with the list of certificates satisfying
8 the at least one inactive criterion; and
9 carrying out the processing operation on the second CRL only if the identity
10 of the latest CRL having differences with the list of certificates satisfying the at least
11 one inactive criterion is more recent than the first CRL.
- 12
- 13 10. The method according to claim 9, wherein the processing operation
14 comprises storing the list of digital certificates satisfying the inactive criterion.
- 15
- 16 11. The method according to claim 9, wherein the processing operation
17 comprises storing the list of digital certificates satisfying the inactive criterion as a
18 part of a database.
- 19
- 20 12. The method according to claim 9, wherein the processing operation
21 comprises filtering the list of digital certificates based on inactive criteria.
- 22
- 23 13. The method according to claim 9, wherein the processing operation
24 comprises authenticating a digital certificate against the second CRL.
- 25
- 26 14. The method according to claim 9, wherein the at least one inactive criterion
27 comprises at least one of a hold status criterion, an expired status criterion and a
28 revoked status criterion.
- 29
- 30

1 15. The method according to claim 9, wherein the first and second CRL are
2 received over an electronic communication medium.

3
4 16. An electronic storage medium storing instructions which when executed on
5 a programmed processor carry out the method of using a digital certificate
6 revocation list according to claim 9.

7
8

1 17. A data structure, stored on a computer readable storage medium or
2 transported over an electronic communication medium, for a digital certificate
3 revocation list (CRL), comprising:

4 a list of digital certificates satisfying at least one inactive criterion;
5 a CRL identifier; and
6 an identity of a latest CRL having differences with the list of digital
7 certificates satisfying the inactive criterion.

8
9 18. The data structure according to claim 17, wherein the CRL identifier
10 comprises a sequentially assigned number.

11
12 19. The data structure according to claim 17, wherein the at least one inactive
13 criterion comprises at least one of a hold status criterion, an expired status criterion
14 and a revoked status criterion.

15
16 20. The data structure according to claim 17, wherein the identity of a latest
17 CRL having differences with the list of digital certificates satisfying the inactive
18 criterion comprises an extension to an ASN.1 standard CRL.